IN THE UNITED STATES PATENT OFFICE

Shimon GRUPER et al.
U.S. Patent Application Serial No. 08/937,883
Filed September 25, 1997
SOFTWARD APPLICATION ENVIRONMENT

September 5th , 2000

DECLARATION IN SUPPORT OF PETITION UNDER 37 CFR 1.131

I, the undersigned, Shimon Gruper, of Hanoter 17, Kiryat Haim, Israel, affirm as follows:

1. I am the Vice President of Aladdin Knowledge Systems Ltd. (hereinafter "the Company"), the assignee of U.S. Patent Application Serial Number 08/937,883 (hereinafter "the Application"). I am also one of the inventors of the invention described and claimed in the Application.

2. It has been explained to me by the Company's patent attorneys and agents from the firm of Sanford T. Colb & Co. that the Application has been rejected by the Examiner on grounds that the invention claimed therein was disclosed prior to the creation of the invention by the present inventors. According to the Examiner, all the features recited in claims 1-3, 6-9, and 13-18 of the Application were explicitly or inherently disclosed in a document dated March 17, 1997 and attributed to Secure4U, and the features recited in claims 4, 5 and 10-12 were obvious at the time the claimed invention was made in view of the Secure4U document in combination with additional art.

3. As will be explained hereinbelow, the Applicants can provide evidence demonstrating conception of the claimed invention prior to March 17, 1997, and diligence thereafter in the reduction of the invention to practice. However, before presenting such evidence, I must express my puzzlement to the basis for the Examiner's rejection. The Examiner's rejection, as I understand it, is based on a document submitted by the Applicants' representative in support of Applicants' petition to make special. This document, a copy of which is enclosed herein as Appendix A, is a printout of Secure4U's web page as it appeared on April 28, 1998. This date is after the filing date of the Application. It is therefore unclear to me how the Examiner arrived at the date of March 17, 1997, since the document submitted by the Applicants' representative was not printed on March 17, 1997 but rather more than a year later, and the Examiner did not provide a copy of the document which according to the Examiner was published on March 17, 1997 and discloses all of the elements of the claimed invention.

4. Without derogating from the foregoing and without prejudice, enclosed herewith as Appendices B, C, D and E are copies of documents from February 1997. These documents were written by one of the present inventors, Mr. Sergey Korabelnikov, and summarize the capabilities of the invention as conceived by the inventors. The documents were written while Mr. Korabelnikov, myself, and the other inventors were employees of Eliashim, and the project was called InterSafe

project. The project was subsequently renamed the eSafe project, and the Company purchased the eSafe product line from Eliashim. In the following paragraphs, I will explain how Appendices B-E demonstrate conception of the elements of the invention, as claimed in the independent claims of the Application (claims 1-3, 8-9, and 13-18), prior to March 17, 1997. I note that at the time the documents in Appendices B, C, D and E were written, the product was referred to by the inventors as "InterSafe".

5. Claim 1 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 1. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
>
> [a] an identifier for identifying an application to be run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application, and
>
> [d] an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level.

[a] *an identifier for identifying an application to be run*

This is described *inter alia* in Appendix D. See particularly page 1, Section 2, especially 2.1, 2.2 and 2.7. → these sections are about detecting apps that are already running

[b] *a listing associated with at least one of said applications to be run*

This is described *inter alia* in Appendices C and D. See particularly page 1, section 4 of Appendix C and page 2, sections 4 and 5, especially section 4.3, of Appendix D. ↳ no listing ↳ no listing

all of these sections have nothing to do with sectors

[c] *said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application*

This is described *inter alia* in Appendices C and D. See particularly page 3 of Appendix C and page 2, sections 4 and 5, especially section 4.2 of Appendix D. ↳ just describes setting security levels for unprotected apps

[d] *an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level.*

This is described *inter alia* in Appendix D. See particularly page 2, section 4.

Thus the invention claimed in claim 1 of the Application was conceived prior to March 17, 1997.

6. Claim 2 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 2. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
>
> [a] an identifier for identifying an application to be run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level,
>
> [d'] an enforcement device, for preventing said at least one application from accessing an identified sector of said storage device at any level higher than said associated access level, and
>
> [e] a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt with said user, and if found acceptable then including said higher level of access in said listing.

Elements [a], [b], and [c] are identical to the corresponding elements recited in claim 1. As for elements [d'] and [e]:

[d'] *an enforcement device, for preventing said at least one application from accessing an identified sector of said storage device at any level higher than said associated access level*
This is described *inter alia* in Appendix D. See particularly page 2, section 4.

[e] *a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt with said user, and if found acceptable then including said higher level of access in said listing*
This is described inter alia in Appendix D. See particularly pages 1-2, sections 1, 4 and 7, especially sections 4.5 and 7.3.

Thus the invention claimed in claim 2 was conceived prior to March 17, 1997.

7. Claim 3 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 3. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
>
> [a] an identifier for identifying an application to be run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level,

> [d'] an enforcement device, for preventing said at least one application from accessing an identified sector of said storage device at any level higher than said associated access level, and
>
> [e'] a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt against a predetermined configuration, and if found acceptable then including said higher level of access in said listing.

Elements [a], [b], and [c] are identical to the corresponding elements recited in claim 1, and element [d'] is identical to the corresponding element recited in claim 2. As for element [e']:

[e'] *a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt against a predetermined configuration, and if found acceptable then including said higher level of access in said listing.*

This is described inter alia in Appendix D. See particularly pages 1-2, sections 1, 4 and 7, especially sections 4.5, 4.6 and 7.3.

Thus the invention claimed in claim 3 was conceived prior to March 17, 1997.

8. Claim 8 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 8. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
>
> [a] an identifier for identifying at least one application to be run, [a'] said at least one application being adapted to call at least one other application to run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,
>
> [d] an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and
>
> [f] wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

Elements [a], [b], [c] and [d] are identical to the corresponding elements recited in claim 1. As for element [f]:

[f] *wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.*

This feature is inherently disclosed in Appendices B-E, in that both Windows 95 and Microsoft Internet Explorer are provided as examples, and both of these are programs that run other programs.

Thus the invention claimed in claim 8 was conceived prior to March 17, 1997.

9. Claim 9 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 9. A computer connected to a network, said computer comprising
>
> [g] a storage device for storing data,
>
> [h] a transmission device for sending data from said computer to said network,
>
> [i] a listing of controlled data which should not be sent to said network,
>
> [j] a comparison device adapted to compare data sent to said transmission device with said controlled data, and
>
> [k] a prevention device for preventing data corresponding to said controlled data being sent automatically to said network.

Elements [g] and [h], are inherent in any computer connected to a network. Elements [i], [j] and [k] can be found, inter alia, in Appendix D, particularly section 6 and 7.

Thus the invention claimed in claim 9 was conceived prior to March 17, 1997.

10. Claim 13 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 13. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
>
> [a] an identifier for identifying at least one application to be run, [a'] said at least one application being adapted to call at least one other application to run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,

> [d] an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and
>
> [e] a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt with a user, and if found acceptable then including said higher level of access in said listing.
>
> [f] wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

Elements [a], [a'], [b], [c], [d], [e] and [f] are identical to the corresponding elements recited in claims explicated above.

Thus the invention claimed in claim 13 was conceived prior to March 17, 1997.

11. Claim 14 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 14. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
>
> [a] an identifier for identifying at least one application to be run, [a'] said at least one application being adapted to call at least one other application to run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,
>
> [d] an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and
>
> [e'] a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt against a predetermined configuration, and if found acceptable then including said higher level of access in said listing,
>
> [f] wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

Elements [a], [a'], [b], [c], [d], [e'] and [f] are identical to the corresponding elements recited in claims explicated above.

Thus the invention claimed in claim 14 was conceived prior to March 17, 1997.

12. Claim 15 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 15. A computer connected to a network, said computer comprising
>
> [g] a storage device for storing data sectorwise,
>
> [h] a transmission device for sending data from said computer to said network,
>
> [i] a listing of controlled data which should not be sent to said network,
>
> [j] a comparison device adapted to compare data sent to said transmission device with said controlled data, and
>
> [k] a prevention device for preventing data corresponding to said controlled data being sent automatically to said network,
>
> said computer further comprising
>
> [a] an identifier for identifying an application to be run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application, and
>
> [d] an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level.

Elements [a], [b], [c], [d], [g], [h], [i] [j] and [k] are identical to the corresponding elements recited in claims explicated above.

Thus the invention claimed in claim 15 was conceived prior to March 17, 1997.

13. Claim 16 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 16. A computer connected to a network, said computer comprising
>
> [g] a storage device for storing data sectorwise,

> [h] a transmission device for sending data from said computer to said network,
>
> [i] a listing of controlled data which should not be sent to said network,
>
> [j] a comparison device adapted to compare data sent to said transmission device with said controlled data, and
>
> [k] a prevention device for preventing data corresponding to said controlled data being sent automatically to said network,
>
> said computer further comprising
>
> [a] an identifier for identifying an application to be run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device and associating with each identified sector an access level,
>
> [d'] an enforcement device, for preventing said at least one application from accessing an identified sector of said storage device at any level higher than said associated access level, and
>
> [e] a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt with a user, and if found acceptable then including said higher level of access in said listing.

Elements [a], [b], [c], [d'], [e], [g], [h], [i] [j] and [k] are identical to the corresponding elements recited in claims explicated above.

Thus the invention claimed in claim 16 was conceived prior to March 17, 1997.

14. Claim 17 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 17. A computer connected to a network, said computer comprising [g] a storage device for storing data sectorwise, [h] a transmission device for sending data from said computer to said network, [i] a listing of controlled data which should not be sent to said network, [j] a comparison device adapted to compare data sent to said transmission device with said controlled data, and [k] a prevention device for preventing data corresponding to said controlled data being sent automatically to said network, said computer further comprising
>
> [a] an identifier for identifying at least one application to be run, [a'] said at least one application being adapted to call at least one other application to run,
>
> [b] a listing associated with at least one of said applications to be run, [c] said listing identifying different sectors of said storage device

> and associating with each identified sector an access level required by said application,
>
> [d] an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and
>
> [f] wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

Elements [a], [a'], [b], [c], [d], [f], [g], [h], [i] [j] and [k] are identical to the corresponding elements recited in claims explicated above.

Thus the invention claimed in claim 17 was conceived prior to March 17, 1997.

15. Claim 18 of the Application reads as follows (bracketed letters have been inserted for ease of reference):

> 18. A computer connected to a network, said computer comprising [g] a storage device for storing data sectorwise, [h] a transmission device for sending data from said computer to said network, [i] a listing of controlled data which should not be sent to said network, [j] a comparison device adapted to compare data sent to said transmission device with said controlled data, and [k] a prevention device for preventing data corresponding to said controlled data being sent automatically to said network, said computer further comprising
>
> [a] an identifier for identifying at least one application to be run, [a'] said at least one application being adapted to call at least one other application to run,
>
> [b] a listing associated with at least one of said applications to be run, [c]said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,
>
> [d] an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and
>
> [e'] a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt against a predetermined configuration, and if found acceptable then including said higher level of access in said listing,
>
> [f] wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then

identifying a listing associated with said at least one application for use with said enforcement device.

Elements [a], [a'], [b], [c], [d], [e'], [f], [g], [h], [i] [j] and [k] are identical to the corresponding elements recited in claims explicated above.

Thus the invention claimed in claim 18 was conceived prior to March 17, 1997.

16. As to claims 6 and 7, it is an inherent feature of the claimed invention as conceived that the invention stops querying when reset because when the system is reset all processing is stopped. Thus the invention claimed in claims 6 and 7 was conceived prior to March 17, 1997.

17. With respect to the claims 4, 5, and 10-12, these claims stand rejected over the Secure4U reference in view of additional references. Claim 4 depends from claim 2, claim 5 depends from claim 3, claim 10 depends from claim 1, claim 11 depends from claim 8, and claim 12 depends from claim 9. In view of the analysis above demonstrating that the invention claimed in each of claims 1, 2, 3, 8 and 9 was conceived prior to March 17, 1997, the combination of the Secure4U publication and additional publications cannot sustain the rejection of claims 4, 5, and 10-12.

18. From February 1997 until September 25, 1997, I worked as part of a team that was assigned to work full-time to reduce the invention to practice.

19. On September 25, 1997, the Application was filed in the USPTO.

20. Furthermore, page 4 of Appendix D shows "Time Table Milestones", i.e. target dates for actual reduction to practice of the invention and development of a commercial product in accordance with the Application. Except for the release of a commercial product (i.e. "Release 1 of Corporate version"), all the deadlines listed took place within about two weeks of the target date: code design review ("CDR") took place around February 23, 1997; code for the program to implement the invention ("Code Completion") was completed around March 31, 1997; a first beta version of a program in accordance with the invention ("Release 1", which was not released to the public) was completed around April 14, 1997, and a second beta version of the program in accordance with the invention ("Release 2", which was not released to the public) was completed around June 2, 1997. The first commercial product was released around early November, 1997.

21. Thus the Applicants were diligent from conception to both constructive as well as actual reduction to practice of the invention.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application of any patent issued thereon.

S. GRUPER

Shimon Gruper
Hanoter 17
Kiryat Haim
September , 2000